ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR CHECKING DIGITAL SIGNATURES AND CARD WITH MICROCIRCUIT FOR USING THE METHOD

To check a digital signature, using a microcircuit card (53), the microcircuit being designed to receive and to process requests to check digital signatures, the process comprises storing in a memory in the microcircuit (53) a certificates table (5, 5') containing digest forms of authorized public keys, and a phase (2) of checking a digital signature consisting of: receiving (21) by the microcircuit the digital signature ($Sig(Ai_p,M)$ to be checked and a public key ($A1_p$) corresponding to a private key that was used to generate the digital signature to be checked; calculating (22) a digest form ($Hash(A1_p)$) of the received public key, searching (23) for the calculated digest form of the public key in the certificates table (5, 5'), and decrypting (25) the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.